PRIVACY IMPACT ASSESSMENT

Diplomatic Security - Antiterrorism Activity - Training Management System

1. Contact Information

> **A/GIS Deputy Assistant Secretary**
> Bureau of Administration
> Global Information Services

2. System Information

(a) **Name of system:** Diplomatic Security - Antiterrorism Activity - Training Management System

(b) **System acronym:** DS-ATA-TMS

(c) **Bureau**: Diplomatic Security

(d) **iMatrix Asset ID Number:** 273697

(e) **Child systems and iMatrix Asset ID Number (if applicable):** N/A

(f) **Reason for performing PIA:**

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(g) **Explanation of modification (if applicable):**

3. Purpose

(a) **Describe the purpose of the system**

The Office of Antiterrorism Assistance (DS/ATA) is responsible for the administration of the Antiterrorism Assistance Program, which trains civilian security and law enforcement personnel from friendly governments in police procedures used for counterterrorism. DS/ATA assesses the training needs of these partner nations (civilian security and law enforcement personnel from friendly governments), develops the curriculum, and provides the resources to conduct the training utilizing its own training experts, as well as those from other Federal, state, and local law enforcement agencies, police associations, and private security firms and consultants. The four key purposes of the TMS system are: delivery of DS/ATA training courses, interactions, and materials; tracking DS/ATA training completions and interactions; management of DS/ATA training resources to include personnel, facilities, and materials; and providing training workflows and scheduling for DS/ATA training.

(b) **List the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:**

DS/T/ATA Employees – Contracted Instructors (U.S. Citizens):
- First Name
- Last Name
- Business Contact Information (Work Email, Work Phone Number, Work Address, Work Title)
- Personal Phone Number
- Personal Email Address
- Personal Address
- Date of Birth
- Emergency contact (name and personal or work phone number)
- Substantive Individual Personnel Information:
- Date of Last Medical Screening
- Date of Last Background Screening
- Date of Last Emergency Medical Technician (EMT) Certification
- Completion of the DS/T/ATA Refresher Course
- Completion of Active Shooter Course; and
- Passport Number and Expiration Date

DS/T/ATA Employees – Non-Instructors (U.S. Citizens):
- First Name
- Last Name
- Department of State Email Address
- Non-Instructor roles include: Program Managers; System Administrators; Training Delivery Coordinator, Point-of-Contacts (POCs); Budget POCs; Logistics POCs; Instructional System, Designer POCs; Virtual Information Specialist POCs; Assessment Monitor Unit, POCs; Executive Management POCs; and Contract Vetting Specialist POCs

Foreign National Students (Non-U.S. Citizens):
- First Name
- Last Name
- Gender
- Date of Birth
- Post

The remainder of this PIA will focus on the PII maintained on U.S. persons.

(c) How is the PII above collected?

DS/T/ATA Employees – Contracted Instructors: PII is obtained and collected directly from the Contracted Instructor using the Instructor/Mentor/Advisor Biographic Application form.

1. The Contracted Instructor completes the Instructor/Mentor/Advisor Biographic Application form.

2. The Contracted Instructor emails the completed form to the Contract Vetting Specialist;
3. The Contract Vetting Specialist conducts a review of the PII; and
4. The Contract Vetting Specialist manually enters the PII into DS-ATA-TMS.

DS/T/ATA Employees – Non-Instructors: PII is obtained and collected directly from the DoS OpenNet Global Access List (GAL), which the System administrator manually enters DS-ATA-TMS.

(d) What is/are the intended use(s) for the PII?

The PII in the DS-ATA-TMS application is used to document course/consultation assignments, determine qualifications to instruct, to document contracted instructors' deployments to their required course/consultation, to document students' attendance at a course/consultation, staff information to assign role permissions, as well as emergency contact information.

(e) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

☒Yes ☐ No

If no, please explain:

4. Authorities and Records
(a) What are the specific legal authorities and/or agreements that allow the information to be collected?

- The Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. § 4801 et seq., as amended; and
- The Foreign Assistance Act of 1961, 22 U.S.C. § 2349aa et. seq., as amended.

(b) If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security numbers.

N/A

(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)?

☒ Yes, please indicate relevant System of Records Notice (SORN) below.

- SORN Name and Number:

  STATE-36 Security Records 12/15/2015

If no, explain how the information is retrieved without a personal identifier.

(d) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

☐ Yes   ☒ No

If yes, please notify the Privacy Office at Privacy@state.gov.

(e) List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system?

Schedule number (e.g., (XX-587-XX-XXX)):
a. DAA-0059-2018-0003-0008
b. DAA-0059-2018-0003-0006

Length of time the information is retained in the system:
a. Temporary. Cut-off upon conclusion of course review or when course is discontinued. Destroy 5 years after cut-off but no later than 30 years if required for business use.

b. Temporary. Cut-off at end of calendar year of final action. Destroy/delete 3 years after cut-off but no later than 10 years if required for business use.

5. Data Sources, Quality, and Integrity

(a) What categories of individuals below originally provide the PII in the system? Please check all that apply.

☐ Members of the public (U.S. persons which includes U.S. citizens or LPRs)
☒ U.S. government employees/contractor employees
☒ Other (people who are not U.S. citizens or LPRs)

(b) Do the individuals listed in 5(a) provide PII on individuals other than themselves? Please check all that apply.

☒ Members of the public
☐ U.S. government employees/contractor employees
☐ Other
☐ N/A

(c) What process is used to determine if the PII is accurate?

DS/T/ATA Employees – Contracted Instructors: PII is obtained and collected directly from the Contracted Instructor using the Instructor/Mentor/Advisor Biographic Application form. It is the responsibility of the Contracted Instructor to ensure the accuracy of the information they provide.

DS/T/ATA Employees – Non-Instructors: PII is obtained directly from the DoS OpenNet Global Access List (GAL) and assumed accurate.

Since both entity's information is assumed accurate, there are no data checks to confirm its accuracy.

(d) What steps or procedures are taken to ensure the PII remains current?

DS/T/ATA Employees – Contracted Instructors: The Contracted Instructor provides updated PII to the Contract Vetting Specialist (ATA Staff) whenever changes are needed, and the Contract Vetting Specialist makes the changes in DS-ATA-TMS.

DS/T/ATA Employees – Non-Instructors: PII is obtained directly from the DoS OpenNet Global Access List (GAL) and assumed current upon upload. Non-Instructors are responsible for notifying ATA-TMS Application Administrators of any necessary updates.

(e) Was the minimization of PII in the system considered?

☒ Yes   ☐ No

If no, please explain.

(f) Does the system use information, including PII, from commercial sources?

☐ Yes   ☒ No

If yes, please list the commercial sources.

(g) Is the information, including PII, collected from publicly available sources?

☐ Yes   ☒ No

If yes, please list the publicly available sources.

(h) Does the system analyze the PII stored in it?

☐ Yes   ☒ No

If yes:

      (1) What types of methods are used to analyze the PII?

      (2) Does the analysis result in new information?

      (3) Will the new information be placed in the individual's record?

      (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

(i) If the system will use test data, will it include real PII?

☐ Yes ☐ No ☒ N/A - this system does not use test data

If yes, please provide additional details.

6. Redress and Notification

(a) Explain whether a notice is provided to the record subject at the point of collection of their information.

DS/T/ATA Employees – Contracted Instructors: The Instructor/Mentor/Advisor Biographic Application form that is used to obtain Contracted Instructor information has an approved Privacy Act Statement (PAS) on the first page.

DS/T/ATA Employees – Non-Instructors: PII is obtained directly from the DoS OpenNet Global Access List (GAL), thus notice is not provided by ATA-TMS.

(b) Are opportunities available for record subjects to decline to provide the PII?

☐ Yes ☒ No

If no, please explain why not.

DS/T/ATA Employees - Contracted Instructors have the opportunity to decline to provide their PII.

DS/T/ATA Employees – Non-Instructors do not since their information is pulled directly from the DoS OpenNet Global Access List (GAL). It is the GAL's responsibility to receive consent upon their initial collection of the information.

(c) Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?

☐ Yes ☒ No

If yes, please explain.

(d) What procedures allow record subjects to gain access to their information?

DS/T/ATA Employees – Contracted Instructors: Contracted Instructors are not authorized access to DS-ATA-TMS. All PII is only populated by ATA Staff. Contracted Instructors may contact ATA Staff, such as their Training Coordinator, to verify the PII maintained on them in DS-ATA-TMS.

DS/T/ATA Employees – Non-Instructor: Non-instructors access the system and their PII with single sign on via OpenNet (GoBrowser and GoVirtual).

Further, the Department's Privacy Act practices allow for record subjects to gain access to their information by contacting the Department for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-36. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

(e) Are procedures in place to allow a record subject to correct or amend their information?

☒ Yes   ☐ No

If yes, explain procedures and how record subjects are notified.

DS/T/ATA Employees – Contracted Instructors: Contracted Instructors do not have direct access to DS-ATA-TMS; however, there are procedures in-place to allow Contracted Instructor PII to be corrected. Contracted Instructors complete a second Instructor/Mentor/Advisor Biographic Application form and submit it to the Contract Vetting Specialist. The Contract Vetting Specialist will then correct the inaccurate or erroneous information in the DS-ATA-TMS application.

DS/T/ATA Employees – Non-Instructor: Non-Instructors must email the ATA-TMS Application Administrator to make any updates or changes to their information.

If no, explain why record subjects are not able to correct their information.

7. Sharing of PII

(a) To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(b) For each of the entities in 7(a), list the PII from 3(b) that will be transmitted.

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(c) For each of the entities in 7(a), what is the purpose for transmitting the information?

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(d) For each of the entities in 7(a), list the methods by which the information will be transmitted.

Internal (within the Department)	External (outside of the Department)
N/A	N/A

(e) For each of the entities in 7(a), what safeguards are in place for each method of internal or external transmission?

Internal (within the Department)	External (outside of the Department)
N/A	N/A

8. Security Controls

(a) How is all of the information in the system secured?

The information in the DS-ATA-TMS application is secured with the following safeguards:

• Connection to the DS-ATA-TMS application is first through the use of Hypertext Transfer Protocol (HTTP) via the Internet.
• The HTTP port then automatically routes the user through the use of Hypertext Transfer Protocol Secure (HTTPS) to the DS-ATA-TMS application.
• All network traffic is HTTPS-encrypted using Federal Information Processing Standard (FIPS) approved encryption and uses Transport Layer Security (TLS) 1.2. The database is stored on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) volumes that are encrypted in place with FIPS-approved Advanced Encryption Standard 256(AES-256) level encryption.
• Access to the DS-ATA-TMS application is limited to either federated authorization via Personal Identity Verification (PIV) card and Security Assertion Markup Language (SAML), yearly training is taken that includes data privacy topics.
• Inherited security controls from the Envisage (SaaS) software.
• Inherited security controls from the AWS-GovCloud (IaaS) network and physical security controls; and
• A Standard Operating Procedure (SOP) for DS-ATA-TMS System Administrators has been established to provide guidance on handling PII.

(b) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud

☐ Other federal agency equipment or cloud
☐ Other
  - If you did not select "Department-owned equipment," please specify.

DS-ATA-TMS is stored on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) volumes that are encrypted in place with FIPS-approved Advanced Encryption Standard 256 (AES-256) level encryption.

(c) In the table below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.

Role	What does the Role do?	What PII does the Role have access to?	What rights to the PII does this user have (Read-only, edits, etc.)	How does the role initially obtain access?	Who approves the roles access?
Application Administrator	Maintains application.	Access to all PII	Edit	Permissions were granted when the application first launched. For subsequent needed access, new Application Administrators must receive access from an existing Application Administrator, or alternatively, through the DS-ATA-TMS system vendor (Vector Solutions) by request via email.	Application Administrators have full control access to the application upon program implementation. For subsequent needed access, an existing Application Administrator can provide access or the System Owner in DS/T/ATA approves the vendor, via email, to provide access.
Contractor Verification	Edit access to instructor	Edit access to all PII	Edit	This role receives	Direct government

Specialist (CVS)	person profiles			access from the Application Administrator	supervisor of individual approves and Application Administrators implement.
Program Manager (PM)	Creates deliveries and reviews, approves, rejects workflows	Access to all PII	Read	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Training Coordinator (TC)	Edits deliveries and reviews, approves, rejects workflows	Access to all PII	Read	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Budget Specialist (Budget)	Read deliveries and reviews, approves, rejects workflows	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Assessment & Monitoring Unit (AMU)	Runs reports and has access to students and instructors	Access to all PII	Read	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Operations Coordinator (OpsCo)	Read access to deliveries	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement

Procurement & Logistics (Logistics)	Read and edit access to deliveries	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Executive Management (EX)	Read access to deliveries and reports	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Branch Chief	Read access to deliveries and reports	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Visual Information Specialist (VIS)	Read access to deliveries and delivery templates	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Functional User	Edit personnel assignments	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement
Instructional System Designer (ISD)	Develops and updates curriculum	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application

					Administrators implement
Reader	Read access to deliveries and reports	None	None	This role receives access from the Application Administrator	Direct government supervisor of individual approves and Application Administrators implement

(d) After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.

For access to this system, management approval is required; approval is based on position as well as a need to know. Audits are completed every month by system administrators to remove access to the system of employees who no longer have a need to know.

(e) Have monitoring, recording, auditing safeguards, and other controls been put in place to prevent the misuse of the information?

☒ Yes   ☐ No

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒ Yes   ☐ No

(g) Privacy Related Training Certification
- Do all OpenNet users of this system take the course PA318 Protecting Personally Identifiable Information biennially?

  ☒ Yes   ☐ No

- Do all OpenNet users of this system take the course PS800 Cybersecurity Awareness Training annually?

  ☒ Yes   ☐ No

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

  ☐ Yes   ☒ No

  If yes, please list the related trainings here: